Exhibit E

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

17 MAG 3734

In the Matter of a Warrant for All Content and Other Information for the Google account associated with Email Address joshschulte1@gmail.com, Maintained at Premises Controlled by Google, Inc. and Google Payment Corp.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Google, Inc. and Google Payment Corp. (collectively "Google")

The Federal Bureau of Investigation (the "FBI" or the "Investigative Agency")

1. Warrant. Upon an affidavit of Special Agent Jeff D. Donaldson of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe that content information maintained at premises controlled by Google associated with the email address joshschulte1@gmail.com contains evidence, fruits, and instrumentalities of a crime, all as specified in Attachment A hereto. Accordingly, Google is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on Google within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which Google is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that Google shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Google may disclose this Warrant and Order to an attorney for Google for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on Google; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

May 17, 2017
Date Issued

3:42 PM
Time Issued

S/Gabriel W. Gorenstein

THE HONORABLE GABRIEL W. GORENSTEIN
United States Magistrate Judge
Southern District of New York

Attachment A

I. The Target Account and Execution of Warrant

This warrant is directed to Google, Inc. and Google Payment Corp. (collectively, "Google" or the "Provider") and applies to all content and other information within Google's possession, custody, or control that is associated with the email address joshschulte1@gmail.com (the "**Target Account**").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to Google. Google is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by Google

To the extent it is within Google's possession, custody, or control, Google is directed to produce the following information associated with the **Target Account**:

a. Search History. All data concerning searches run by the user of the **Target Account**, including, but not limited to, the content, date, and time of the search.

b. Google+ Photos and Content. All data concerning Google+ Photos, including all albums, photos, videos, and associated metadata for each file, as well as all Google+ posts, comments, profiles, contacts, and information relating to Google+ Circles.

c. Google Drive Content. All files and folders in the Google Drive associated with the **Target Account**.

d. Google Voice. All records, voicemails, text messages, and other data associated with Google Voice.

l. *Transactional records.* All transactional records associated with the **Target Account**, including any IP logs or other records of session times and durations.

m. *Customer correspondence.* All correspondence with the subscriber or others associated with the **Target Account**, including complaints, inquiries, or other contacts with support services and records of actions taken.

n. *Advertising ID and DoubleClick records.* The Advertising IDs assigned to devices associated with the **Target Account**, and all DoubleClick or other records of internet activity associated those Advertising IDs.

o. *Preserved records.* Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by Google in order to locate:

(i) any evidence, fruits, and instrumentalities of the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (the "National Security and Computer Crime Offenses"), for the time period March 14, 2017 to the present; and

(ii) any evidence, fruits, and instrumentalities of (i) violations of Title 18, United States Code, Section 2252 (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) and Title 18, United States Code, Section 2252A (activities relating to material constituting or containing child pornography) (the "CP Offenses"); and (ii) violations of Title 17, United States Code, Section 506 and Title 18, United States Code, Section 2319 (criminal infringement of a copyright) (the "Copyright Offenses") (collectively, with the National Security and Computer Crime Offenses and the CP Offenses, the "Subject Offenses"), for the time period May 17, 2007 through the present.

Such evidence, fruits, and instrumentalities of the Subject Offenses include the following:

a. Evidence of the identity(s) of the user(s) of the **Target Account** as well as other coconspirators in contact with the **Target Account**;

b. Evidence relating to the geolocation and travel of the user(s) of the **Target Account** at times relevant to the Subject Offenses;

c. Evidence relating to the participation in the Subject Offenses by the users of the **Target Account** and others;

d. Evidence concerning financial institutions and transactions used by the users of the **Target Account** in furtherance of the Subject Offenses;

e. Communications evidencing crimes, including but not limited to correspondence with others relating to the Subject Offenses;

f. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user of the **Target Account**; and

g. Passwords or other information needed to access any such computers, accounts, or facilities.

17 MAG 3734

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and Other Information for the Google account associated with Email Address joshschulte1@gmail.com, Maintained at Premises Controlled by Google, Inc. and Google Payment Corp.	**TO BE FILED UNDER SEAL** **Agent Affidavit in Support of Application for Search Warrant**

Application for a Search Warrant for Stored Electronic Communications

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

JEFF D. DONALDSON, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") assigned to the New York Field Office, and have been employed by the FBI since 2010. I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from 2010 to present. In the course of my duties as a Special Agent, I am responsible for investigating offenses involving espionage and related violations of law, including unauthorized retention, gathering, transmitting or losing classified documents or materials; unauthorized removal and retention of classified documents or materials; illegally acting in the United States as a foreign agent; other national security offenses; and the making of false statements. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure or retention of classified information, as well as my training in counterintelligence operations, I am familiar with the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and

may choose to harm the United States by misusing their access to classified information. I am also familiar, though my training and experience with the use of computers in criminal activity and the forensic analysis of electronically stored information.

2. **Basis for Knowledge.** This Affidavit is based upon my participation in the investigation, my examination of reports and records, and my conversations with other law enforcement agents and other individuals, as well as my training and experience. Because this Affidavit is being submitted for the limited purpose of obtaining the Requested Information, it does not include all the facts that I have learned during the course of this investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. In addition, unless otherwise indicated, statements by others referenced in this Affidavit were not necessarily made to me, but may have been provided to me by someone else to whom I have spoken or whose report I have read (and who in turn may have had either direct or indirect knowledge of the statement). Similarly, unless otherwise indicated, information in this Affidavit resulting from surveillance does not necessarily set forth my personal observations, but may have been provided to me by other law enforcement agents who observed the events, and to whom I have spoken or whose report I have read.

II. The Target Account

3. I make this Affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 directed to Google, Inc. and Google Payment Corp. (collectively "Google" or the "Provider"), headquartered in Mountain View, CA, for all content and other information associated with the following "**Target Account**": the Google account associated with the email address joshschulte1@gmail.com, which is maintained and controlled by Google.

4. On or about March 14, 2017, the Honorable Barbara C. Moses issued a search warrant for all content and other information associated with the **Target Account** (the "March 14 Target Account Search Warrant"), which was issued in connection with an investigation into the unlawful retention and dissemination of classified materials. Following the execution of the March 14 Target Account Search Warrant, the investigation has revealed that the **Target Account** is likely to contain evidence, fruits, and instrumentalities of offenses involving child pornography and copyright infringement, in addition to offenses relating to the retention and dissemination of classified materials.

5. Based on returns obtained pursuant to the March 14 Target Account Search Warrant, as well as other evidence encountered in this investigation as described below, this application seeks a search warrant (a) directing Google to provide all content and information associated with the **Target Account**; (b) authorizing the review of content and other information associated with **Target Account** for evidence, fruits, and instrumentalities of the offenses relating to the unlawful retention and dissemination of classified materials (described further below and in Attachment A) from March 14, 2017 to the present; and (c) authorizing the search of content and other information associated with of the **Target Account** for evidence, fruits, and instrumentalities of offenses relating to child pornography and copyright infringement (described further below and in Attachment A) from May 17, 2007 through the present.

6. Based on my training, experience, and participation in this investigation, I know the following about Google:

a. Google offers email and other Internet-based services to the public. Among other things, Google allows subscribers to maintain email accounts under the domain name gmail.com. A subscriber using Google's services can access his or her email account from any

computer connected to the Internet, and can link any variety of Google's other Internet-based services to his/her Gmail account.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include

records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google's website).

v. *Linked Accounts.* Google also typically maintains records of other Google accounts likely sharing a common owner with a target account. Google may identify such accounts through the use of "cookie" files that reveal when the same web browser is used to log in to multiple Google accounts, or by comparing subscriber information across its records to identify accounts that share, *e.g.*, a recovery email account or phone number.

vi. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

vii. *Preserved records.* Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f).

c. In addition, subscriber information for the **Target Account** indicates that the subscriber of the **Target Account** has activated additional online Google Services, and, accordingly, the Provider also maintains, among other things, the following records and information with respect to the **Target Account**:

i. *Google Drive.* Google provides users with a certain amount of free "cloud" storage, currently 15 gigabytes, through the service called "Google Drive" (users can purchase a storage plan through Google to store additional content). Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content "in the cloud," that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet.

Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files

ii. *Google Docs.* Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called "Google Docs." Users can use Google Docs to create online documents that can be stored on or saved to the user's Google Drive. Users can also download such documents in various formats, such as a Microsoft Word document (e.g., ".docx"), an OpenDocument Format (".odt"), Rich Text Format (".rtf"), a PDF document (".pdf"), or Plain Text document (".txt").

iii. *Google Photos.* Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or "Exif") data, and can include GPS location information for where a photo or video was taken.

iv. *Google Calendar.* Google provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

v. *YouTube content.* Google allows subscribers to maintain linked YouTube accounts, a global video-sharing website that allows users to upload and share videos

with public on the Internet. Registered users can upload an unlimited number of videos and add comments to videos.

vi. *Google Chats and Google Hangouts content.* Google allows subscribers to engage in "chat" sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user's email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user's email and chat content.

vii. *Location history data.* Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or "apps") or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user's location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device's most recent location data in connection with a Google account.

viii. *Android Services.* Google also maintains information relating to Android, as it relates to an account. Android is a mobile operating system that is developed by Google, and is used on a variety of touchscreen mobile devices, such as smartphones and tablet computers. Google retains information related to the Android device associated with an account, including the IMEI (the International Mobile Station Equipment Identifier), MEID (the Mobile Equipment Identifier), device ID, Google-assigned Advertising ID, and/or serial number of the devices. Each of those identifiers uniquely identifies the device used. One device may be associated with multiple different Google and Android accounts, and one Google or Android account may be associated with multiple devices.

ix. *Google Voice.* Google provides a telephone service that provides call forwarding and voicemail services, voice and text messaging.

x. *Google Payments and Wallet.* Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, and the transfer of money by subscribers using their Google Gmail address or phone number, among other features.

xi. *Web History.* Google maintains searches and account browsing activity, from Chrome, Google's proprietary web browser, as well as other Google applications. Some of this data is obtained through Google's advertising business, also known as DoubleClick.

III. Jurisdiction to Issue Requested Warrant

7. Pursuant to Title 18, United States Code, Sections 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as Google, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

8. A search warrant under Section 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

9. When the Government obtains records under Section 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as

the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

IV. The Subject Offenses

10. For the reasons detailed below, I believe that there is probable cause that the **Target Account** contains evidence, fruits, and instrumentalities of (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B) (the "National Security and Computer Crime Offenses"); (ii) violations of Title 18, United States Code, Section 2252 (possession, transportation, receipt, distribution, production, and reproduction of sexually explicit material relating to children) and Title 18, United States Code, Section 2252A (activities relating to material constituting or containing child pornography) (the "CP Offenses"); and (iii) violations of Title 17, United States Code, Section 506 and Title 18, United States Code, Section 2319 (criminal infringement of a copyright) (the "Copyright Offenses") (collectively, with the National Security and Computer Crime Offenses and the CP Offenses, the "Subject Offenses").

A. Terminology

11. The term "computer," as used herein, is defined as set forth in 18 U.S.C. § 1030(e)(1).

12. The term child pornography is defined in Title 18, United States Code, Section 2256(8) in pertinent part as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct."[1]

13. The terms "Minor," "Sexually Explicit Conduct" and "Visual Depiction" are defined as set forth in Title 18, United States Code, Section 2256.

V. Probable Cause and Request to Search

A. Probable Cause Relating to the National Security and Computer Crime Offenses

14. Based on my review of publicly available material on the Internet, including on the website wikileaks.org ("WikiLeaks"), I know that, on March 7, 2017, WikiLeaks published what it claimed were more than 8,000 documents and files that contained classified information (the "Classified Information") belonging to the Central Intelligence Agency ("CIA"). In its press release accompanying the Classified Information, WikiLeaks further claimed that:

a. The public dissemination of the Classified Information was "the largest ever" unauthorized publication of classified CIA documents.

b. The Classified Information constituted the "first full part" of a series—thus indicating that there would be subsequent publications of additional sensitive CIA information.[2]

c. The "collection" obtained by WikiLeaks amounted to "more than several

---

[1] *See also Ashcroft* v. *Free Speech Coalition*, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

[2] On or about March 24, 2017, March 31, 2017, April 7, 2017, April 14, 2017, April 21, 2017, April 28, May 5, 2017, and May 12, 2017 WikiLeaks released additional batches of documents that it claimed were also obtained from the CIA.

hundred million lines of code" and revealed the "entire hacking capacity" of the CIA, including various malware, viruses, and other tools used by the CIA.

15. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that:

a. The information that WikiLeaks claimed was classified CIA information—that is, the Classified Information—was at the time of its disclosure, in fact, classified CIA information.

b. Specifically, the Classified Information was created and maintained by one specific group within the CIA which is responsible for various computer engineering activities, including the development of computer code (the "CIA Group"). That CIA Group exists within a larger CIA component (the "CIA Component"). In March 2016, less than 200 employees were assigned to the CIA Group.

c. The Classified Information was maintained by the CIA Group on an isolated local-area computer network (the "LAN").[3] Only employees of the CIA Group had access to the LAN on which the Classified Information was stored.[4]

---

[3] In its press release announcing the publication of the Classified Information, WikiLeaks stated that the Classified Information originated from "an isolated, high-security network."

[4] Prior search warrant applications in connection with this investigation set forth that a preliminary analysis had concluded that the Classified Information was likely copied from a back-up server to which the same three systems administrators likely had access. The information that the Classified Information was likely recovered from an automated back-up file to which only systems administrators likely had access was first received by the FBI on or about March 22, 2017. As set forth herein, an investigation is ongoing as to whether the stolen data was in fact back-up data taken from the automated back-up. But, nevertheless, the current assessment remains that the copying of the data, regardless of the data's original location, would likely have required systems administrator access of the type maintained by TARGET SUBJECT JOSHUA ADAM SCHULTE. Accordingly, I respectfully submit that the precise location from where the Classified Information was taken—whether from an automated back-up file or from a non-back-up computer file—does not affect the probable cause underlying the prior search warrant applications.

i. An isolated network, such as the CIA Group's LAN, is a network-security structure by which the isolated network is physically separated (or "air-gapped") from unsecured networks, such as the public Internet.

ii. Accordingly, such isolated networks, like the LAN, cannot be accessed from the public Internet, but rather only through those computers which are physically connected to the isolated network.

iii. The CIA Group's LAN, and each of its component parts, was maintained in heavily secured governmental facilities, which include multiple access controls and various other electronic and physical security measures.

d. Based on a preliminary analysis of the timestamps associated with the latest (or most recent) creation or modification date associated with the Classified Information, it appears that the Classified Information was copied from the LAN in or about March 2016.

e. The duplication and removal from the LAN of the Classified Information and its subsequent public dissemination via WikiLeaks was not authorized by the United States government.

f. The unauthorized disclosure of the Classified Information could—at a minimum—reasonably be expected to cause serious damage to the national security of the United States. *See* Executive Order 13526; 18 C.F.R. § 3a.11(a)(2).

g. The Classified Information is national defense information and its disclosure could reasonably be expected to be used to the injury of the United States and to the advantage of a foreign nation. *See* 18 U.S.C. § 793(d) & (e).

16. I know, based on my conversations with other law enforcement agents and others, that TARGET SUBJECT JOSHUA ADAM SCHULTE was employed as a computer engineer by

the CIA—specifically in the CIA Group—from in or about May 2010 through on or about November 10, 2016, when he resigned from the CIA. Based on those conversations, I understand the following about the nature of SCHULTE's employment with the CIA, in substance and in part:

a. During SCHULTE's more than six years working in the CIA Group, his responsibilities included, among other things, developing computer code for specific projects, including projects explicitly described in the Classified Information. SCHULTE had a skill set that enabled him to write computer code designed to clandestinely copy data from computers.

b. As part of his responsibilities with the CIA Group, in or about March and early April 2016, SCHULTE was one of three system administrators for the LAN. Among other things, that meant that he was one of three employees responsible for maintaining the LAN, and for controlling the access of other CIA Group employees.

c. These three systems administrators also had "super-user" access to the LAN, which allowed them broader access to programs, files and servers.

17. Based on my conversations with law enforcement officers and others, including individuals with an expertise in computer systems, and knowledge of the LAN, and my conversations with individuals who have conducted preliminary forensic analyses of the LAN and its related computer systems, I understand the following, in substance and in part:

a. Preliminary analysis suggests that the wholesale access to, and subsequent copying of, the Classified Information would likely have required systems administrator access of the type described above.[5]

[5] I describe this as a "preliminary analysis" because analysis of the precise origin of the Classified Information is ongoing, and therefore the conclusions drawn from the preliminary analyses to date may be subject to modification once the analysis has been concluded. For example, among the facts that the FBI and CIA continue to analyze and verify is the precise number of individuals with "super-user" access who would have had access to the Classified Information during the relevant

b. The publicly released Classified Information originally published by WikiLeaks, based on a preliminary review, appears to contain the names and/or pseudonyms of, *inter alia,* multiple CIA employees—including two of the three aforementioned LAN systems administrators. SCHULTE's name, on the other hand, apparently was not published in the Classified Information. Thus, SCHULTE was the only one of the three systems administrators who was not publicly identified via WikiLeaks's first publication of the Classified Information.

c. The other two individuals who served in March 2016 as systems administrators for the CIA Group's LAN remain employed by the CIA. SCHULTE resigned from the CIA in November 2016, as described in detail below.

18. Based on my conversations with other law enforcement agents and others, my review of documents prepared by such law enforcement agents or obtained from the CIA, I know that SCHULTE has alleged that, on or about March 1, 2016, another CIA Group co-worker had made a threat against him. Based on those conversations and that review of documents regarding SCHULTE's threat allegations against his former co-worker, I understand the following, in substance and in part:

a. The CIA conducted an investigation into the incident, at the conclusion of

---

time period, which in and of itself is in part dependent upon the mechanism or route by which the Classified Information was obtained. Information the FBI received on April 5, 2017 revealed that there is a possibility that this number could have been slightly lower or slightly higher than the initial estimates set forth in prior search warrant affidavits submitted in the course of this investigation, and that such variation depends on the route through which the Classified Information was accessed. While there may have been multiple mechanisms to gain access to the Classified Information, the preliminary assessment is that the most likely routes to acquiring that information would have required systems administrator access. Notwithstanding that fact, it is, of course, also possible that an employee who was not a designated systems administrator could find a way to gain access to the Classified Information (*e.g.*, an employee could steal and use—without legitimate authorization—the username and password of a designated systems administrator, or an employee lacking systems administrator access could, at least theoretically, gain access to the Classified Information by finding a "back-door" to it).

which SCHULTE expressed deep unhappiness about the way that CIA responded to the alleged threat.

b. SCHULTE threatened legal action against the CIA for its handling of the situation, and repeatedly stated that he felt that he was being punished by CIA management for reporting the alleged threat incident.

c. SCHULTE informed CIA security that, if "forced into a corner" he would proceed with a lawsuit against the CIA. He also repeatedly threatened that he or his lawyer would go to the media.

d. In addition, CIA security learned that SCHULTE had removed an internal CIA document from CIA facilities that related to his complaints to the CIA concerning its handling of the alleged threat, despite being told multiple times by CIA security officials not to do so. On or about April 4, 2016, SCHULTE and the other CIA employee were reassigned to different offices within the CIA Group in response to SCHULTE's allegations.

e. Around the time of his reassignment to another branch within the CIA Group, and at least in part because of his new responsibilities, many of SCHULTE's administrator privileges on the LAN were revoked, and he was no longer permitted to serve as a systems administrator in the CIA Group's LAN.

f. At approximately the same time, *i.e.*, on or about April 4, 2016, SCHULTE's computer access to a specific developmental project ("Project-1") was also revoked. Until his reassignment, SCHULTE had been the CIA Group employee with principal responsibility for Project-1. Upon SCHULTE's transfer, principal responsibility for Project-1 was

transferred to another CIA Group employee, who received computer access to Project-1.[6]

19. I know from my review of publicly available material on the Internet, including WikiLeaks.org, that Project-1 was one of a small group of CIA projects and capabilities that WikiLeaks highlighted explicitly by name in its March 7, 2017 press release that accompanied the online publication of the Classified Information.

20. Based on my involvement in this investigation and my conversations with other FBI agents involved in this investigation, I know that on or about March 14, 2017, pursuant to the March 14 Target Account Search Warrant described above in paragraph 4, Google produced information, including a history of TARGET SUBJECT JOSHUA ADAM SCHULTE's Google searches (the "Google Search(es)" or "Search(es)").

21. The Google Searches, which are described in detail below, were conducted using the **Target Account** (joshschulte1@gmail.com), which the investigation has revealed belongs to SCHULTE.

22. Based on my review of those Google Searches, and conversations with law enforcement agents and others, as well as my own training and experience, I know that on or about April 4, 2016, SCHULTE conducted a Google Search that led him to visit a webpage entitled in part "Detecting USB insertion/Removal in C++ non-GUI application."[7] I understand, based on my training, experience, and conversations with others, that "Detecting USB insertion/[r]emoval" likely relates to the function by which a computer recognizes—or does not recognize—that an external device has been connected to it via its USB port. (A USB port is a standard connection

[6] SCHULTE retained read-only access to Project-1 (but not the ability to alter the code) and the ability to copy the computer code associated with it in order to support another project for which he had responsibility.

[7] Both C++ and non-GUI (which stands for graphical user interface) are references to standard types of computer programming language or code, used, inter alia, by aspects of the LAN.

interface used to connect devices to a computer, including—among numerous other peripheral items—a portable computer storage device.)

23. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand the following, in substance and in part:

a. On or about April 11, 2016, approximately one week later, SCHULTE unilaterally, and without authorization, logged onto the CIA Group's LAN and reinstated his own administrator privileges.

b. CIA Group management did not discover that SCHULTE had personally re-instituted his administrator privileges to the LAN without permission until on or about April 14, 2016.

24. Based on my review of the Google Searches, I know that on April 12 and 13, 2016 (*i.e.*, the time period between when SCHULTE reinstated his access to the LAN and FBI's discovery of that unauthorized reinstatement), SCHULTE conducted a series of searches apparently designed to gather information about copying a large quantity of data from one computer storage device to another, including but not limited to the following:

a. On or about April 12 and 13, 2016, in the evening,[8] SCHULTE conducted the following Google Searches, among others:

i. "windows command line copy all files subdirectories";

ii. "windows copy all files and subdirectories"; and

iii. "windows back files xcopy or robocopy"

[8] The Google search warrant returns list the times of the searches in "UTC" or coordinated universal time, which is the same as Greenwich Mean Time. Accordingly, the dates and times of the Google Searches described herein have been adjusted to Eastern Standard Time (*i.e.*, the time zone where SCHULTE conducted the Google Searches).

I understand, based on my training, experience, and conversations with others, that "robocopy" and "xcopy" each refer to computer commands that allow a user to copy multiple computer files—or entire computer directories (and all their contents)—from one computer storage location to another. For example, this command would be used to copy files and folders, *en masse*, from one network to another, from one computer to another, or from a computer network onto a portable hard drive. According to publicly available materials published by Microsoft, the "robocopy" function would allow a user "to mirror the contents of an entire folder hierarchy across local volumes or over a network. . . . Robocopy is a powerful tool, capable of moving, copying, and deleting files and folders faster than you can say 'Whoops.'" In addition, the Robocopy command allows a user to copy an entire file storage directory sporadically, rather than all at one time. It does that by enabling the copying process to proceed in increments and re-start from where it left off, rather than requiring a user to start the copying process over again from the beginning.

b. On the following day, April 13, 2016, SCHULTE conducted Google Searches apparently designed to gather information about the speed of various portable, external computer hard drives, such as "thumb drives" and "flash drives," which are computer memory storage devices that connect to a computer typically via a USB port, including searches for:

i. "thumbdrive copy speed";

ii. "flash drive transfer rate"; and

iii. "flash drive read speeds"

c. Later in the day on April 13, 2016, within minutes of conducting the Google Searches regarding portable hard drive speeds, SCHULTE also conducted another Google Search apparently designed to identify the most efficient way to copy units of computer data: "optimal reading chunk size c++". I know, based on my training, experience and conversations with other

law enforcement agents with technical expertise regarding computers, that:

i. Computers store, read and write data in units that are sometimes referred to as "blocks" or "chunks." When data is copied, each block or chunk is separately read, copied and written from the original storage location to the destination storage location. These data blocks or chunks can be of varying sizes. Accordingly, the speed and efficiency of copying data can be affected by the size of each block or chunk of data.

ii. After conducting the above-mentioned Google Search ("optimal reading chunk size c++"), SCHULTE visited websites relating to issues such as "what is the ideal memory block size to use when copying."

25. Based on my review of the Google Searches, I understand that on or about April 15, 2016, SCHULTE conducted the following Google Search relating specifically to software running on the CIA Group's LAN: "[] admin view restricted pages."[9] After conducting the search, SCHULTE visited websites that related to ways to restrict the ability of even other Systems Administrators to view aspects of the LAN. (SCHULTE conducted the same search again thirteen days later, on or about April 28, 2016.)

26. Based on my conversations with law enforcement officers and others with knowledge of SCHULTE's personnel file, I understand the following, in substance and in part:

a. On or about April 18, 2016, approximately four days after the CIA had learned of SCHULTE's unauthorized reinstatement of his systems administrator privileges, SCHULTE received notice regarding CIA policies against personnel restoring their own access to privileges or computer networks after those accesses have been revoked.

[9] The brackets redact out the proprietary name of the specific commercially available software program that was running on the CIA Group's LAN.

b. SCHULTE signed an acknowledgment that he understood that "individuals are not permitted to personally attempt and/or renew their previous authorizations [including administrator privileges] to any particular [computer] system." That notice further instructed SCHULTE: "do not attempt to restore or provide yourself administrative rights to any project and/or system for which they have been removed."

27. Based on my review of the Google Searches, and my conversations with other law enforcement officers who have reviewed the Searches, I understand the following, in substance and in part:

a. Also on or about April 18, 2016 (*i.e.*, the same day he was required to sign the acknowledgement of CIA policies), SCHULTE conducted various Google Searches regarding copying files on a computer network, including "copying multiple [] large files." After conducting this search, SCHULTE visited a website titled, in part, "how to copy a large number of files quickly between two servers."

b. Less than a week later, on or about April 24, 2016, SCHULTE conducted a Google Search for a "SATA adapter." Based on my training, experience and conversations with others, I understand that such an adapter is used to connect a computer hard drive to a computer externally, via USB connection. In other words, by connecting an internal drive to another computer via that computer's external USB port, a SATA adapter allows an internal computer hard drive to be used instead as a portable, external memory drive.

c. On or about April 24, 2016, SCHULTE conducted multiple Google Searches for how to "partition" or divide a computer hard drive up, in order to move files from one storage location on the computer to a separate drive or portioned location.

d. On or about April 28, 2016, SCHULTE again conducted a Google Search

relating specifically to software running on the CIA Group's LAN: "[] admin view restricted pages," which was identical to the Search, described above, he conducted on April 15, 2016—four days after restoring his own administrator access to that very software program without authorization.

e. On the evening of Saturday, April 30, 2016, SCHULTE conducted numerous Google Searches apparently relating to the deletion of computer data, including possibly his own Google Searches, which searches included the following:

i. "google history";

ii. "google view browsing history";

iii. "western digital disk wipe utility"; and

iv. "Samsung ssd wipe utility"

I know, based on my training, experience and conversations with others, that "[W]estern [D]igital" is the name of one of the largest providers of computer storage hardware (such as portable hard drives), and that "wipe utility," or wipe drive utilities are, based on the description on Western Digital's website, designed to "erase all the data on a hard drive." I further know, based on my training, experience and conversations with others, that Samsung SSD is a reference to a brand (Samsung) of solid-state drives, which is a type of portable computer hard drive.

28. Based on my involvement in this investigation, and my conversations with other law enforcement officers involved in this investigation, I know the following, in substance and in part:

a. On March 15, 2017, the Honorable Barbara C. Moses issued a search warrant (the "March 15 Residence Search Warrant") for a Manhattan apartment located at 200 East 39th Street, Apartment 8C, New York, New York 10016, in which SCHULTE has resided

since shortly after his resignation from the CIA in November 2016 (the "Residence").[10]

b. Pursuant to the search conducted on that same day, law enforcement officers recovered, among other things, numerous computer storage devices with the capacity to store at least more than ten terabytes of data, including multiple Western Digital hard disk drives (themselves totaling multiple terabytes[11] of storage space) and at least one Samsung SSD solid state external hard drive.[12] As noted immediately above, these are the two brands of hard drive which SCHULTE specifically searched for "wipe utilities"—programs designed to completely erase data from the drives—on the evening of April 30, 2016.[13]

29. Based on my review of the Google Searches, and my conversations with other law enforcement officers who have reviewed the Searches, I understand the following, in substance and in part:

a. At approximately 3:20 a.m. in the early morning hours of May 1, 2016 (*i.e.*, approximately five hours after conducting the Google Searches regarding the wiping of hard drives described in Paragraph 21(e) above), SCHULTE visited a website entitled in part "how can I verify

---

[10] Previously, on March 13, 2017, Judge Moses had issued a search warrant for the same premises. The Government sought a second search warrant for an overt search of the premises because the March 13 search warrant had been executed covertly on or about March 14, 2017 and agents were not able to complete the search.

[11] I know, based on my training, experience and conversations with others, that one terabyte of data is roughly equivalent to one-thousand gigabytes of data or one-million megabytes of data. Put differently, one terabyte of data is roughly equivalent to more than 85 million word processing pages.

[12] Those computer devices are in the process of being analyzed.

[13] In addition, pursuant to the search, agents recovered from SCHULTE's apartment, internal correspondence from the CIA that appears, based on a preliminary analysis, to contain classified information (though *not* the Classified Information), including, *inter alia*, the names of CIA employees, and code names of specific CIA Group programs. I know, based on my training, experience and conversations with others, that removing and storing classified information in one's own home is generally prohibited.

that a 1tb file transferred correctly." I know, based on my training, experience and conversations with others, that "1tb" likely refers to 1 terabyte of data.

b. Three days later, on or about May 4, 2016, SCHULTE again conducted multiple Google Searches apparently related to the permanent deletion of data from a computer storage device, including "western digital disk wipe utility" and "can you use dban on ssd." Based on my training, experience and conversations with others, I understand that:

i. "SSD" is an acronym for "solid-state drive" a kind of computer memory storage device.

ii. "dban" is an acronym that stands for "Darik's Boot and Nuke," a computer software program that is designed, according to various websites selling the software, to "securely wipe[] the hard disks of most computers. DBAN is appropriate for bulk or emergency data destruction." According to one popular technology website, CNET.com: "use DBAN only if you want to completely eradicate any trace of data on a hard drive. This is the ultimate in data shredding—there's no recovery once you've used it."

c. Starting two days later, May 6, 2016, and again on May 8, 2016, SCHULTE conducted multiple Google Searches apparently designed to research the anonymous transmission of data on the Internet, through the use of so-called "private trackers," which are non-public Internet sites set up to privately transfer large quantities of data from one computer to another, as well as through "The Onion Router" or "TOR," which allows for anonymous communications on the Internet via a worldwide network of linked computer servers, and multiple layers of data encryption.

d. On May 6, 2016, SCHULTE conducted multiple Google Searches apparently relating to ways to transfer data between computers anonymously, including searches

for "trackers," "trackers torrent," and "private trackers." Based on my training, experience and conversations with others, I understand that trackers or torrent trackers are computer code (or a "protocol") that connects computers on the Internet to each other in order to facilitate the transfer of large files over the Internet. I further understand that "private trackers" are trackers that are not publicly accessible, but rather that require authorization by an administrator to use the tracker to share files. After conducting the Google Search for "private trackers," SCHULTE visited a website entitled "opentrackers.org," which claims that its private tracker can be used "to avoid detection & bypass anti-piracy/site blocking."[14]

e. On May 8, 2016, SCHULTE conducted multiple Google Searches apparently related to the use of The Onion Router (or TOR) to anonymously transfer encrypted data on the Internet. For example, SCHULTE searched for "setup for relay," "test bridge relay," and "tor relay vs bridge." Each of these searches returned information regarding the use of interconnected computers (or relays) on TOR to convey information, or the use of a computer to serve as the gateway (or bridge) into the TOR network of relays.

30. Based on my conversations with law enforcement officers and others with knowledge of SCHULTE's personnel file and computer access, I understand the following, in substance and in part:

a. On May 26, 2016 (*i.e.*, less than three weeks after he conducted Google Searches related to the use of TOR as described above), and notwithstanding the warnings described above, SCHULTE made an official request that he again be given full access to Project-

[14] Trackers and torrent trackers are often used in the transfer of large media files, including video and audio. The investigation to date has indicated that, in addition to the activity set forth in this section, SCHULTE also appears to have been engaged in the sharing of large media files, including, among other things, movies and music. Accordingly, it is at least possible that certain of these searches, as well as others described herein, could relate to those activities.

1.

b. Before receiving an official response to that request, SCHULTE requested access from another employee who, apparently without proper vetting, granted SCHULTE the requested full access to Project-1.

c. On the same day, SCHULTE used that newly obtained access to, unilaterally and without authorization, revoke the computer access permissions of all other CIA Group employees to work on Project-1.

d. Once this conduct was discovered, SCHULTE was issued a letter of warning that stated, "You were aware of the policy for access and your management's lack of support for you to retain administrative privileges, but nonetheless you took steps to deliberately violate that policy and gain those privileges." It continued by warning SCHULTE that any future violations would result in "further administrative action of a more severe nature." After receiving the letter of warning, SCHULTE disagreed with some of its conclusions and consequently refused to sign the form.

31. Based on my review of the Google Searches, and my conversations with other law enforcement officers who have reviewed the Searches, I understand the following with respect to TARGET SUBJECT JOSHUA SCHULTE's searches related to WikiLeaks, in substance and in part:

a. For the approximately six years between at least August 2010 and August 3, 2016, he conducted no searches for WikiLeaks.

b. But, beginning on August 4, 2016, SCHULTE initiated numerous Google Searches for WikiLeaks and related terms, and visited more than 200 pages that he apparently found as a result of those searches.

c. Between August 4 and August 22, 2016, SCHULTE conducted Searches for "wikileaks" at least eleven times. Pursuant to those Google Searches, he read dozens of articles regarding WikiLeaks, though he appears never to have actually visited the WikiLeaks.org Internet website.[15]

d. Between August 2016 and March 14, 2017, he searched "wikileaks" at least a dozen additional times, and read hundreds of online articles and publications regarding WikiLeaks. He apparently first visited the WikiLeaks.org website on March 7, 2017—the date of the release of the Classified Information.

e. In addition to the numerous searches for "wikileaks" which commenced on August 4, 2016, SCHULTE also conducted multiple related Searches, including: prior to the March 7, 2017 release of the Classified Information, "assange" (Julian Assange is the founder and "editor-in-chief" of WikiLeaks.org), "snowden its time," "wikileaks code," and "wikileaks 2017"—and after the March 7, 2017 release of the Classified Information, "wikileaks public opinion," and "officials were aware before the WikiLeaks release of a loss of sensitive information."

32. Based on my review of the Google Searches, and my conversations with other law enforcement officers who have reviewed the Searches, I further understand the following, in substance and in part:

a. On August 1, 2016, SCHULTE conducted a Google Search for "create temporary email," and, three seconds later, visited the website www.throwawaymail.com. Based

[15] I know, based on my training, experience, and conversations with others, that, among many other reasons, one reason a person might search for "wikileaks" but never visit the website is because the act of visiting a website can leave a trail that a particular IP address visited the website. Accordingly, one reason (perhaps among many) for repeatedly searching "wikileaks" but not visiting the WikiLeaks.org website, would be to avoid leaving behind a footprint of one's visit.

on my training, experience, conversations with others, and review of documents, I know that "throwawaymail.com" is an Internet website that randomly generates an anonymous email address for a user without any registration; that random and anonymous email address can immediately receive and send emails, but automatically expires within a very short period of time (approximately 48 hours).

b. On August 10, 2016, SCHULTE conducted a Search for "tails," and then, two seconds later, visited the website "https://tails.boum.org." I know, based on my training, experience, conversations with others, and review of that website, that "tails" is an acronym for "the Amnesic Incognito Live System," that works in conjunction with TOR (described above) to ensure anonymous connections on the Internet and therefore will leave no digital footprint of the internet websites visited by someone using the system.[16] The WikiLeaks.org website also lists "tails" as one of its "partner organizations."

c. On August 14, 2016, SCHULTE searched various topics regarding employment litigation and disputes, including filing a lawsuit against one's boss (*e.g.* "can you sue your boss"), one's employer (*e.g.* can i sue my employer for unfair treatment"), and the "EEOC." (Less than an hour after conducting those Searches, SCHULTE searched "tor.")

d. On September 1 and 5, 2016, SCHULTE repeatedly searched, "what is a mole." I know, based on my training and experience that, among other meanings, a "mole"

[16] News reporting indicates that Edward Snowden used the tails system in connection with his transfer of allegedly classified documents to various news outlets. *See* Out in the Open: Inside the Operating System Edward Snowden Used to Evade the NSA, Wired, April 14, 2014, *available at* https://www.wired.com/2014/04/tails/ (last accessed Mar. 31, 2017); The ultra-secure Tails OS beloved by Edward Snowden gets a major upgrade, PC World, Jan. 27, 2016, *available at* http://www.pcworld.com/article/3026721/linux/the-ultra-secure-os-beloved-by-edward-snowden-gets-a-major-upgrade.html (last accessed Mar. 31, 2017).

generally refers to a spy working inside a country's security, military or intelligence services.

33. Based on my conversations with law enforcement officers and others familiar with TARGET SUBJECT JOSHUA SCHULTE's employment history with the CIA, including his security clearances and related investigations, I understand the following, in substance and in part:

a. In approximately August 2016, as part of a standard background reinvestigation of SCHULTE for the purpose of renewing his security clearances, the CIA conducted interviews of multiple CIA Group colleagues. Among other things:

b. Some (but not all) colleagues independently reported that SCHULTE's demeanor with his management and colleagues, and his commitment to his work, changed markedly for the worse in or around February 2016.

c. Multiple colleagues stated that SCHULTE had indicated that he felt aggrieved by the CIA in a number of respects. Some also reported that they believed SCHULTE to be untrustworthy and potentially subject to outside coercion. (Other colleagues made no such report and, indeed affirmatively reported that they believed that SCHULTE was, in fact, trustworthy.)

d. Some (but not all) colleagues also reported that SCHULTE's security practices were lax, and that SCHULTE tended not to abide by security guidelines he deemed inconvenient—particularly guidelines concerning when and what kinds of media or data (such as external drives) could be connected or uploaded to CIA computer systems.[17]

34. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know in substance and in part that, in

[17] As described herein, external drives can be connected to computers and files in order to allow users to move files from the computers onto the portable external drives.

connection with and preceding SCHULTE's November 2016 resignation from the CIA:

a. Approximately one month prior to his resignation, on October 12, 2016, SCHULTE, using his CIA email account, sent an email to another CIA Group employee at that employee's official email account. The subject line of the email stated, "ROUGH DRAFT of Resignation Letter *EYES ONLY*." The email contained a letter entitled "Letter of Resignation 10/12/16" and addressed to "To whomever it may concern" ("Draft Resignation Letter"). I know from reviewing the Draft Resignation Letter, which spanned approximately three single-spaced pages, the following:

i. SCHULTE began the letter by stating, in substance and in part, that he had "always been a patriot" and would "obviously continue to support and defend this country until the day that I die," but that "from this day forward" he would "no longer do so as a public servant."

ii. SCHULTE claimed that he believed that the CIA Group management had unfairly "veiled" CIA leadership from various of SCHULTE's previously expressed concerns, including concerns about the network security of the CIA Group's LAN. SCHULTE continued: "That ends now. From this moment forward you can no longer claim ignorance; you can no longer pretend that you were not involved."

iii. SCHULTE explained that he was resigning from the CIA because CIA Group management had, among other things, "ignored" issues he had raised about "security concerns" and had attempted to "conceal these practices from senior leadership," including that the CIA Group's LAN was "incredibly vulnerable" to the theft of sensitive data. He claimed that one named CIA Group manager had ignored his security concerns and "later attempt[ed] to evade responsibility and blame the decentralized and insecure [CIA Group computing] environment

entirely on me."[18]

iv. Specifically, SCHULTE wrote that inadequate CIA security measures had "left [the CIA Group's LAN] open and easy for anyone to gain access and easily download [from the LAN] and upload [sensitive CIA Group computer code] in its entirety to the [public] internet."

b. It appears that SCHULTE did not, in fact, submit the Draft Resignation Letter to the CIA.

c. On his last day with the CIA (November 10, 2016), SCHULTE did, however, send an internal email to the CIA Office of the Inspector General (OIG) advising that he had been in contact with the United States House of Representatives' Permanent Select Committee on Intelligence regarding his complaints about the CIA (the "OIG Email").

i. In the OIG Email, which SCHULTE labeled "Unclassified," SCHULTE raised many of the same complaints included in the draft "Letter of Resignation 10/12/16," described above, including the CIA's treatment of him and its failure to address the "security concerns" he had repeatedly raised in the past.

ii. Shortly thereafter, CIA security learned that one of SCHULTE's colleagues had witnessed SCHULTE printing the OIG Email, placing it in a folder, and exiting the CIA Component facility where SCHULTE worked. Notwithstanding SCHULTE's labeling of the email as "Unclassified," the CIA subsequently determined that the OIG Email, which SCHULTE removed from the CIA without authorization, did in fact contain classified information.

[18] SCHULTE went on to describe other complaints he had about managers at the CIA. Among other things, SCHULTE described his complaints about the way in which CIA Group management had handled various personnel and disciplinary issues.

35. Based on my involvement in this investigation, and my conversations with other law enforcement officers involved in this investigation and/or my review of reports prepared in the course of this investigation, I understand that the FBI recovered a copy of the November 10, 2016 OIG Email, which contained classified information and which SCHULTE labeled "Unclassified" and removed from a CIA facility, from his residence during the March 15, 2017 search.

36. Based on my conversations with other law enforcement agents and others, and my review of documents, I also understand that, following the March 7, 2017 publication of the Classified Information on WikiLeaks, SCHULTE repeatedly initiated contact, via telephone and text messages, with multiple of his former CIA Group colleagues. Those colleagues reported that contact to government and law enforcement officials. In particular, I know the following regarding SCHULTE's communications in the days following March 7, 2017:

a. In those communications with his former colleagues, SCHULTE repeatedly asked about the status of the investigation into the disclosure of the Classified Information.

b. SCHULTE requested more details on the information that was disclosed.

c. SCHULTE inquired of his interlocutors' personal opinions regarding who, within the CIA Group, each believes is responsible for the disclosure of the Classified Information. SCHULTE also asked what other former CIA Group colleagues are saying about the disclosure.

d. SCHULTE repeatedly denied any involvement in the disclosure of the Classified Information.

e. SCHULTE indicated the he believes that he is a suspect in the investigation of the leak of Classified Information.

37. Furthermore, I have learned that SCHULTE specifically used the **Target Account**, *i.e.*, the account associated with the Gmail account joshshulte1@gmail.com, to make some of the inquiries described above. For example:

a. I know from records previously obtained from Google that, on or about March 7, 2017, when WikiLeaks released the Classified Information, SCHULTE used the Google Voice feature associated with the **Target Account** to send approximately 149 texts to multiple of his former colleagues at the CIA.

b. I have learned from other FBI agents who have spoken with some of SCHULTE's former colleagues at the CIA that SCHULTE, using the Google Voice feature associated with the **Target Account**, also had phone calls with former CIA colleagues, including one telephone call with a former colleague in which he, among other things, inquired of the former colleague's personal opinions regarding who was responsible for the disclosure of the Classified Information and what the person's motivation might be. SCHULTE indicated on this call that he believed that the person responsible was a contractor who disclosed the Classified Information for fame.

c. I have further learned from other FBI agents who have spoken with some of SCHULTE's former colleagues at the CIA that, in a call using the telephone number associated with the **Target Account** on or about March 8, 2017 with the same former colleague, SCHULTE denied his involvement in the disclosure of the Classified Information, indicated his belief that many people suspected him of the disclosure, and relayed a conversation with another acquaintance in which SCHULTE had denied involvement in the disclosure of the Classified Information, but was dissatisfied with the acquaintance's reaction to SCHULTE's denial.

B. Probable Cause Relating to CP Offenses

38. As described above, On March 15, 2017, the Honorable Barbara C. Moses issued a search warrant authorizing a search of SCHULTE's residence in Manhattan—the March 15 Residence Search Warrant. Based on my involvement in this investigation, and my conversations with other law enforcement officers involved in this investigation as well as my review of documents prepared in the course of this investigation, I understand the following, in substance and in part:

a. During the execution of the March 15 Search Warrant, law enforcement officers recovered, among other things, multiple computers, servers, and other portable electronic storage devices (the "Schulte Devices"). Following the seizure of the Schulte Devices, the devices were transported by the FBI for analysis and examination to a U.S. Government facility in Herndon, Virginia, within the Eastern District of Virginia.

b. In the course of searching the Schulte Devices for evidence, fruits, and instrumentalities of the National Security and Computer Crime Offenses, agents discovered a photograph on SCHULTE's desktop computer that appeared to depict child pornography (the "CP Picture"). An agent who is assigned to the Crimes Against Children Squad (the "CACS Agent") reviewed the CP Picture and believed that the CP Picture depicted a naked young child on all fours and what appear to be two adults around her, one of whom appears to be performing a sexual act on the child—oral sex around the child's buttocks. The CACS Agent also believed that the child was a minor based on, among other things, body structure, lack of breast development, and lack of pubic hair.[19]

[19] Based on my conversations with the CACS Agent, I understand that it is possible that the CP Picture (like many photographs of child pornography) could be altered and not a real picture. However, the CACS Agent had only reviewed a printout of the CP Picture. Members of the FBI who analyzed the Desktop Computer have informed me that the CP Picture looks more

c. Following the discovery of the CP Picture, search warrants were issued in the Eastern District of Virginia that expanded the scope of the search of the Schulte Devices to include evidence, fruits, and instrumentalities of the CP Offenses, as well as Copyright Offenses Although the search of the Schulte Devices is ongoing, agents have encountered on one of the Schulte Devices a volume of files (the "Volume"), approximately 54 GB in size, that contains several layers of encryption. Agents have been able to access the encrypted Volume, which contains what appeared to be hundreds of files organized into separate folders. Some of the folders are labeled "downloads," "kids," "old," "other," and "young."[20]

d. One of the files in the Volume is a video with the filename "pthc maryann 2yo suck.mpg." The video depicts a prepubescent girl, estimated to be younger than five years old, with her mouth on an adult's penis. Another file in the Volume, with the filename "real underage fuck cum baby 2yo rape.mpg," is a video that contains multiple scenes. The first scene depicts what appears to be an adult male placing his finger, and later his penis, inside the vagina of a prepubescent girl, estimated to be younger than five years old.

C. Probable Cause for Evidence of Copyright Offenses

39. Based on my conversations with members of the FBI who were involved in searching the Schulte Devices for evidence, fruits, and instrumentalities of the National Security and Computer Crime Offenses pursuant to prior search warrants, I have learned, among other things, that at least one of the servers recovered from SCHULTE's Manhattan residence ("Server-1") has indications that SCHULTE was involved in illegally sharing copyrighted movies over the

---

like an actual photo when viewed on the computer as opposed to when printed. I know that an agent involved in this investigation has viewed the CP Picture on the Desktop Computer and concluded that it is an actual photograph.

[20] The search warrants in the Eastern District of Virginia were issued on or about April 14, 2017 and May 10, 2017.

Internet. Specifically, Server-1's command log (which shows the history of commands sent to Server-1 by the user, likely via a computer connected to Server-1), indicates that SCHULTE participated in the sharing of dozens of movies using torrent trackers.[21] As described above, based on my training, experience and conversations with others, I understand that torrent trackers are computer protocol which connect computers on the Internet to each other in order to facilitate the transfer of large files over the Internet.

40. Based on my training, experience, and my conversations with another FBI agent who has reviewed the public catalog of copyrighted works available through the United States Copyright Office, I know that most, if not all, of the movies that SCHULTE appears to have participated in sharing are copyrighted works registered with the United States Copyright Office. For example, among the many movies that were apparently shared include *Hacksaw Ridge*; *The Revenant*; *Captain America: Civil War*; and *The Hateful Eight*, all of which are copyrighted works currently registered with the United States Copyright Office.

41. Based on my involvement in this investigation as well as my review of reports prepared in the course of this investigation, I understand that in or about March 2017, FBI agents conducted interviews of multiple CIA employees who know SCHULTE, and that, among other things, one of those employees stated that SCHULTE operates a service allowing users to stream movies over the internet (the "Streaming Service") and that SCHULTE manages the accounts of users of the Streaming Service.

[21] Upon viewing the command log, which was searched pursuant to a prior search warrant for evidence regarding the National Security and Computer Crime Offenses, and upon seeing indications of illegal movie sharing, members of the FBI stopped viewing the command log and contacted the U.S. Attorney's Office. A warrant was then obtained to search for evidence, fruits, and instrumentalities of the Copyright Offenses.

42. Based on my review of a telephone that was among the Schulte Devices searched for evidence, fruits, and instrumentalities of the National Security and Computer Crimes Offenses pursuant to the terms of the March 15 Residence Search Warrant, I have learned, among other things, that on or about October 31, 2016, SCHULTE, using a Gmail address associated with the **Target Account**, sent an email to approximately 20 other individuals with the subject line "Pedbsktbll Plex Server Downtime 11/9/2016-1/2017" (the "Email"). In the Email, SCHULTE notifies the recipients that the "server will be down as it relocates to NYC starting 11/9. Thus, you will have the next 9 days to select and download material you may wish to watch during that downtime. Hopefully, the server will be back and running mid to late December – January at the latest." Based on my training, experience, and participation in this investigation, I believe that SCHULTE was referring to the Streaming Service and was alerting users that the service would be unavailable while he moved to New York in late 2016.

* * *

43. I respectfully submit that there is probable cause therefore to believe that the **Target Account** contains evidence, fruits, and instrumentalities of the Subject Offenses. Among other things, I respectfully submit that there is probable cause to establish that SCHULTE is proficient in and makes use of Internet-based computing services, including those offered by the Provider through the **Target Account**.

44. Moreover, based on my training and experience, I know that individuals who engage in the Subject Offenses often use Internet-based services (like the **Target Account**) as a means by which to communicate with co-conspirators as well as means through which not only to transmit but also to store purloined information so that they do not have to carry it on their person. In addition, I know that individuals who engage in the Subject Offenses use Internet-based services

like the **Target Account**, to conduct searches that are relevant to committing or to avoiding detection for crimes such as the Subject Offenses.

45. Finally, I know that individuals who engage in the Subject Offenses oftentimes use Internet-based computing services, like the **Target Account**, to publish purloined information. For example, based on my training and experience and my involvement in this investigation, I know that WikiLeaks is an Internet-based publication and that individuals who provide information to WikiLeaks in the past oftentimes have done so through the use of other Internet-based computing platforms, like the **Target Account** and other services offered by the Providers. Accordingly, when each of these factors is considered in conjunction with the fact of SHCULTE's access to the purloined information, his clear proficiency in computers and computer-programming, his extensive prior use of the **Target Account** related to the commission of the Subject Offenses, and the probable cause establishing SCHULTE's access to and use of the **Target Account**, I respectfully submit that there is probably cause to believe that the **Target Account** will contain evidence, fruits, and instrumentalities of the Subject Offenses.

46. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrants requested herein will be transmitted to the Providers, which will be directed to produce a digital copy of any responsive records to law enforcement personnel within 10 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence,

fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the requested warrants, which shall not be transmitted to the Providers.

47. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all content associated with the **Target Account**. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, to the extent applicable, including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

VI. Request for Non-Disclosure and Sealing Order

48. The existence and scope of this ongoing criminal investigation are not publicly known. As a result, premature public disclosure of this Affidavit or the requested warrants could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. In particular, given that targets of the investigation are known to use computers and electronic communications in

furtherance of their activity, the targets could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation.

49. Accordingly, there is reason to believe that, were the Provider to notify the subscriber(s) or others of the existence of the requested warrants, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person of the existence of the warrant for a period of 180 days from issuance, subject to extension upon application to the Court, if necessary.

50. For similar reasons, I respectfully request that this Affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and Affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

JEFF D. DONALDSON
Special Agent
Federal Bureau of Investigation

Sworn to before me on
this 17th day of May 2017

S/Gabriel W. Gorenstein

THE HONORABLE GABRIEL W. GORENSTEIN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and Other Information for the Google account associated with Email Address joshschulte1@gmail.com, Maintained at Premises Controlled by Google, Inc. and Google Payment Corp.

SEARCH WARRANT AND NON-DISCLOSURE ORDER

TO: Google, Inc. and Google Payment Corp. ("Google")

The Federal Bureau of Investigation (the "FBI" or the "Investigative Agency")

1. Warrant. Upon an affidavit of Special Agent of the FBI and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe that content information maintained at premises controlled by Google associated with the email address joshschulte1@gmail.com contains evidence, fruits, and instrumentalities of a crime, all as specified in Attachment A hereto. Accordingly, Google is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on Google within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which Google is capable of accepting service.

2. Non-Disclosure Order. Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in destruction of or tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that Google shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Google may disclose this Warrant and Order to an attorney for Google for the purpose of receiving legal advice.

3. Sealing. It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on Google; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

3/14/17 — Date Issued

1:11 AM — Time Issued

THE HONORABLE BARBARA MOSES
United States Magistrate Judge
southern District of New York

Attachment A

I. The Subject Account and Execution of Warrant

This warrant is directed to Google, Inc. and Google Payment Corp. (collectively, "Google" or the "Provider") and applies to all content and other information within Google's possession, custody, or control that is associated with the email address joshschulte1@gmail.com (the "Subject Gmail Account").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to Google. Google is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

II. Information to be Produced by Google

To the extent it is within Google's possession, custody, or control, Google is directed to produce the following information associated with the Subject Gmail Account:

a. Search History. All data concerning searches run by the user of the Subject Gmail Accounts, including, but not limited to, the content, date, and time of the search.

b. Google+ Photos and Content. All data concerning Google+ Photos, including all albums, photos, videos, and associated metadata for each file, as well as all Google+ posts, comments, profiles, contacts, and information relating to Google+ Circles.

c. Google Drive Content. All files and folders in the Google Drive associated with the Subject Gmail Account.

d. Google Voice. All records, voicemails, text messages, and other data associated with Google Voice.

e.

f. Google Wallet Content. All data and information in the Google Wallet associated with the Subject Gmail Account.

g. YouTube Content. For any YouTube account associated with the Subject Gmail Account, all subscriber information as well as copies of any videos and associated metadata and any YouTube comments or private messages.

h. Android Content. Any Android device information associated with the Subject Gmail Account, including IMEI/MEID, make and model, serial number, date and IP of last access to Google, and a list of all accounts that have ever been active on the device.

i. Email Content. All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Gmail Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email).

j. Address book information. All address book, contact list, or similar information associated with the Subject Gmail Account.

k. Subscriber and payment information. All subscriber and payment information regarding the Subject Gmail Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

l. Linked accounts. The account identifiers for all accounts linked to the Subject Gmail Accounts, and subscriber records therefore as described in the preceding sub-paragraph,

including but not limited to any account linked to the Subject Gmail Account by registration IP address, "machine" or other cookie, alternate email address, or telephone number.

m. Transactional records. All transactional records associated with the Subject Gmail Account, including any IP logs or other records of session times and durations.

n. Customer correspondence. All correspondence with the subscriber or others associated with the Subject Gmail Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

o. Preserved records. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by Google in order to locate any evidence, fruits, and instrumentalities of violations (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); and (iv) intentionally exceeding authorized access to a computer and thereby obtaining information from a department or agency of the United States,

in violation of Title 18, United States Code, Section 1030(a)(2)(B) (collectively the "Subject Offenses"), including the following:

i. Evidence of the identity(s) of the user(s) of the Subject Gmail Account as well as other coconspirators in contact with the Subject Gmail Account;

j. Evidence relating to the geolocation and travel of the user(s) of the Subject Gmail Account at times relevant to the Subject Offenses;

k. Evidence relating to the participation in the Subject Offenses by the users of the Subject Gmail Account and others;

l. Evidence concerning financial institutions and transactions used by the users of the Subject Gmail Account in furtherance of the Subject Offenses;

m. Communications evidencing crimes, including but not limited to correspondence with others relating to the unauthorized retention, gathering, and transmission of classified documents or materials, and the unauthorized removal and retention of classified documents or materials;

n. Evidence of and relating to computers or other online accounts and facilities (such as additional email addresses) controlled or maintained by the user of the Subject Gmail Account; and

o. Passwords or other information needed to access any such computers, accounts, or facilities.